

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-76412

(P2000-76412A)

(43)公開日 平成12年3月14日(2000.3.14)

(51)Int.Cl'	識別記号	F I	マーク*(参考)
G 0 6 K 19/10		G 0 6 K 19/00	S
G 0 6 F 19/00		17/00	V
G 0 6 T 7/00		G 0 6 F 15/30	3 3 0
1/00			3 5 0
G 0 6 K 17/00		15/62	4 6 0

審査請求 未請求 請求項の数12 書面 (全 8 頁) 最終頁に続く

(21)出願番号 特願平10-281881

(71)出願人 591071230

株式会社ソリトンシステムズ

東京都新宿区新宿2丁目4番3号

(22)出願日 平成10年8月28日(1998.8.28)

(72)発明者 錦田 信夫

東京都新宿区新宿2丁目4番3号 株式会  
社ソリトンシステムズ内

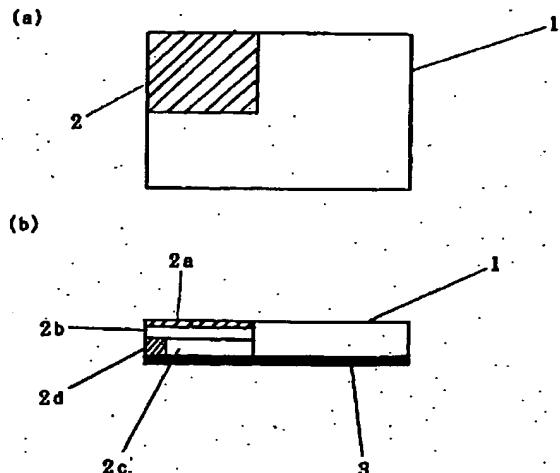
(54)【発明の名称】 指紋認証付電子カード及びその方法

(57)【要約】

【課題】 カードの不正使用を防ぐためカード上に指紋捺印部を設けて暗証番号と併用して本人確認と安全性の向上を可能にする。

【解決手段】 カード1に指紋読み取り部2を設けて指紋パターンの検出を行う。指紋読み取り部2は指紋捺印部2aと指紋読み取りCCDエリアセンサー2b、制御用LSI、2cと外部装置インタフェース部2dより構成する。本人確認のために2より入力した指紋は悪用を防ぐため、所定時間経過後に自動消去する。制御用LSI、2cに格納してある登録指紋パターンと入力した指紋パターンを照合して本人の認証を行う。不正使用が複数回行われた場合制御LSI、2cの機能によって自らカードの機能を使用不可能にするために破壊する。

使用期限が過ぎたカードは自ら内部機能を破壊して再使用を不可能にする。



Best Available Copy

## 【特許請求の範囲】

【請求項1】 銀行カード、クレジットカード、電子マネー等に、本人であることを認証するための指紋捺印部を設け、かつ捺印した指紋は所定時間後に自動消去する事を特徴としたカード。

【請求項2】 請求項1において、カード上に設けた指紋読み取りセンサーは半導体を使用し、かつカード上に制御用LSIを設け、該メモリに登録した指紋パターンと、半導体センサーから入力した指紋パターンと照合する手段を備えた事を特徴とするカード。

【請求項3】 請求項1において、本人確認のための指紋認証と併に暗証番号を併用し、本人識別の精度を向上した事を特徴とするカード。

【請求項4】 請求項2において、カード上の制御用LSIは、メモリ上に登録した指紋パターンと半導体センサーより入力した指紋パターンが一致した場合は一致信号を、一致しない場合は誤り信号をカード上の制御部より出力する事を特徴としたカード。

【請求項5】 請求項2において、該半導体センサーから入力した指紋パターンはメモリに格納後、所定時間経過後に消去する事を特徴としたカード。

【請求項6】 請求項2において、該半導体センサーより入力した指紋パターンは、公衆網を介してデータベースに登録格納してある、該認証の目的のための、指紋パターンをカード読み取り装置に入力の都度、呼び出し照合を行う事を特徴としたカード。

【請求項7】 請求項1においてカード等は所定の期限に達したら、前記カード上の制御LSIによって、内部データ、情報等を破壊して使用不可能にする事を特徴としたカード。

【請求項8】 請求項1においてカードに備えてある指紋捺印部は、指紋パターンの写る事が容易な部材で構成し、写された部材上の指紋を光照射して反射又は、透過光により認識する手段を備えた事を特徴としたカード。

【請求項9】 請求項8において、該カード読み取り装置に捺印した指紋パターンを清掃する部材を備えてカードの決済の都度捺印部の清掃を行い、捺印した指紋パターンを消去する事を特徴としたカード。

【請求項10】 請求項2において登録指紋パターンと捺印した指紋パターン及び暗証番号が一致しない場合、少なくとも複数回の不一致を確認したとき、カード読み取り装置において、カードの没収を行う事を特徴とする事。

【請求項11】 請求項10において、カードの没収と共にカード読み取り装置に備えられたカメラによって不正使用者の容貌等の撮影を行い記憶、保存する事を特徴とする事。

【請求項12】 前記請求項1において、カードは電子財布41に収納して、前記指紋認証手段によって残高又は個人情報等の表示を行う事を特徴とする事。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明はクレジットカード、電子マネー等の本人確認のための指紋認証とその方法に関するものである。

## 【0002】

【従来の技術】マルチメディアが全世界規模に進展する中で、キャッシュレス時代が急速に到来した。マルチメディアの基幹網とも言うべき地球規模の情報ハイウェイ 10 GII (GLOBAL INFORMATION IN FRASTRUCTURE) は21世紀初頭に実用化する。

【0003】カード決済、電子マネーは社会に広く流通し、街角でも家庭でも使用が可能になった。しかし現実には、前記高速情報ハイウェイが整備されても個人確認を暗証番号及びサインのみにたよっている。

【0004】この本人確認方法だと他人に悪用されたり偽造され易く、とても電子マネー、クレジットカードには適しているとは言いがたい。現実にカードによる事故、トラブルは多発していて社会問題となっている。

【0005】暗証番号を盗まれたり、改ざん、あるいは海外でカードを使用して、身に覚えのない請求が来たりする例は後をたたない。

## 【0006】

【発明が解決しようとする課題】従来のカード決済においては暗証番号の盗用や不正使用が絶えなかった。このような悪用を防ぐためには、暗証番号、自筆のサインだけではとても不可能である。近年技術の進歩によって人の眼のアイバターンをカメラに撮って識別する方法も実現している。

【0007】しかし現実には装置が複雑で高価であって、とても容易に家庭などで使えない。まして、街中で、銀行、オフィスでの使用は使い勝手が悪く実用的でない。眼科医院用なら実用化は可能であろう。

【0008】本発明は上記の問題に鑑みてなされたもので、クレジットカード、電子マネーの決済に最も簡便な指紋パターンの照合によって本人確認の精度を向上させて不正使用を防ぐ事を目的としたものである。

## 【0009】

【課題を解決するための手段】上記目的を達成するために本発明のカード及びその方法は以下の構成を備えている。即ちカード上に指紋捺印部を設けて、使用する際本人確認のために指紋の捺印をする。

【0010】電子カードには指紋パターンを認識する半導体エリヤセンサ、制御用LSIが一体となって埋込まれており、制御部メモリには本人登録の指紋パターンが格納してある。決済の際入力した指紋パターンは半導体エリヤセンサで読み取って制御部キャッシュメモリに一時貯える。

50 【0011】入力した指紋パターンと登録してある指紋

パターンの照合は制御部CPUによって行われる。一致、不一致の信号は、カード上の外部装置とのインターフェースを介して出力する。

【0012】入力した指紋パターンは所定時間、例えば5分とか10分間経過したら自動的に消却する。不正使用を防ぐために、落してしまっても他人に使用されないために有効である。

【0013】登録指紋パターンはカード上のメモリではなくカード会社、銀行のデータベースセンターに保管しておいても良い。決済の都度、高速公衆回線を介して決済端末機（カードリーダー）に呼び出して照合しても良い。当然従来からの暗証番号を併用して安全性を確保する。

【0014】また、好ましくは電子カード上にある個人情報又は、電子マネー、銀行カードの場合は残高が表示出来る電子財布41を用意する。ワイシャツのポケットに入るサイズで電子カードを挿入して携帯する事が出来る。必要に応じて指紋パターンを捺印すれば前記内容が電子財布41に表示される。

【0015】また、好ましくは電子カードを、より簡単にするために従来のカード上に指紋捺印部を設けて決済の都度、使用者は捺印して決済端末機に挿入する。決済端末機はカード上の指紋パターンを読み取って、データベースセンターに登録してある指紋パターンと照合する。

【0016】この場合、決済端末機には捺印した指紋を消却するための清浄装置が備えられている。従って決済の都度、捺印した指紋は消却されるから、他人に悪用される心配はない。

【0017】また、好ましくは、カード決済端末機は家庭用FAX付電話器と一体となった構造にしてホーム決済を可能にする事。高齢化社会を迎えて、ショッピング、銀行、郵便局に出向かなくても家庭で用事をすませる事が可能になる。

【0018】また、好ましくは前記電子カードは、複数回不正使用された場合はカード上の制御機能によって内部メモリ上の情報の破壊、制御LSI自体を自動的に壊してしまう機能をもっている事。

#### 【0019】

【発明の実施の形態】以下、添付の図を参照して本発明の実施形態を説明する。

#### 【0020】

【第1の実施形態】各種クレジットカードをはじめ、銀行カード、近年は電子マネーを含めてカードの決済（以下カードと呼ぶ）は普及の段階に達した。インターネットの社会への浸透と共にこの傾向は一段と拍車がかかってきた。

【0021】しかしカード社会の到来と共に困った問題も発生してきた。カード決済に伴う犯罪が急激に増加している事だ。クレジットカードの悪用は手口が年々と

巧妙になってきている。暗証番号の解読による不正使用、カードの偽造は日常化している。要は本人しか使えないようにして、他人が不正使用した場合は没収するとかカード機能を破壊する構造にしておけば問題は解決する。

【0022】従来、クレジットカードのたぐいは変造、偽造が容易であった。テレフォンカードやバチンコカードが大きな社会問題になったのは記憶に新しい。クレジットカードにいたっては使用者のサインだけで決済できるので、落として他人に拾われ不正に使われた例は枚挙にいとまがない。

【0023】その対策として近年、二重の暗証番号を使用するインターネットショッピングの例も出現した。即ち電子財布を開く暗証番号と決済する際の、暗証番号を二重にしてセキュリティを確保している。しかしこれでも完全とは言えない。番号を他人知られてしまえば悪用されてしまう。

【0024】さらに最近実用化されているものに、暗証番号発生器（パターンジェネレータ）を備えた決済装置が登場した。決済機はランダムに発生する暗証番号のパターンジェネレータがあり、決裁者は使用の都度、任意の暗証番号を選んで決済する。これと、パターンジェネレータを備えた決済装置が必要となり、簡単に使える代物ではない。

【0025】本発明はカードに捺印した指紋認識と暗証番号の併用によって、本人確認のセキュリティの向上を計ったものである。カードを盗まれたり、偽造されても、指紋の照合により決済を行うから、暗証番号を他人に知られたり、解読されても悪用の危険は少ない。かつて、使用する本人は決済直前にカード上に指紋の捺印をして決済機、銀行のATM等で本人の確認を行う。カード上に捺印した指紋は、例えば10分後とか15分後の所定時間経過後に自動消去するから、拾われたり偽造されても悪用される心配がない。

【0026】図1は本発明によるクレジットカード等のカードの全体図1を示す。表面上は普通流通しているカードと何ら変らない。図1は図1(a)に示すように、カード1と指紋読取り部、制御部2、それに電池3より構成している。

【0027】図1(b)はカード1の断面図を示す。指紋読取り部2は、透明な部材で構成された捺印部2a、指紋読取りセンサアレイ2b、制御用LSI2c、それに外部装置、例えば銀行のATMとか店舗の決済機36との接続部2dより成る。指紋読取り部2は、例えば米国ペリディコム社の商品名“FPS100”を用いる。“FPS100”は標準CMOSプロセス技術を使用した静電容量型の指紋スキャナチップである。

【0028】制御用LSI2cは、例えば日立製作所商品名“F-ZTAT”マイコンを使用する。“F-ZTAT”マイコンは指紋読取り、本人確認用指紋パター

ンの記憶、本人登録パターンとの照合、本人確認の信号出力、不正使用の場合の誤り信号の出力を行う。外部装置との入出力は制御LSI 2cと一体となったデータバスポートあるいはシリアルポート2dの外部装置インターフェース部によって行われる。

【0029】本カードの特徴は指紋読み取り部2にある。

指紋パターン読み取りエリヤセンサ2b、制御LSI 2cそれに指紋捺印部2aが一体となった構造でカードに埋込まれている。CMOSエリヤセンサ2bと制御LSI 2cは階層構造になっており2bと2c間は絶縁層によって電気的に隔離している。2b、2c、2d間の信号の入出力部は当然絶縁層を介して導体によって接続している。

【0030】図1において電池3はフィルム一次電池を示す。薄さ0.1~0.5mmの薄型で、高イオン導電性高分子固体電解質で実現している。もちろん、従来のコイン電池をカードに埋込んで使用しても良いが、フィルム電池は薄さとパワーと寿命に大きな特徴がある。

【0031】クレジットカード等においては有効期限が定められており、有効期限に寿命をもうけている。カード会社の大部分は新規カードの更新にあたって旧カードの回収を行う場合もあるが、図1(b) 2cの制御LSIによって使用期限に達したら自から内部情報、データ、機能を破壊してしまうのも一方法である。

【0032】銀行カードのように使用期限の決まっていない場合もある。その場合、例えば銀行のATMにカードを挿入した時に、図1(b) 2dの入出力端子の一端に充電端子を設けて、決済中に電位を測定して、充電の必要があれば、決済処理中にATMより充電しても良い。

【0033】図2は制御LSI、2cの内部構成を示す。先にも説明したように指紋読み取り用の透明な部材図1(b)の2aとCMOSエリヤセンサ2bが一体となった構造になっている。エリヤセンサから瞬時に指紋パターンを読み出すために各種のレジスター21、22が効率よく備えてある。

【0034】21はエリヤセンサからサンプリングするためのエリヤセンサの縦方向、横方向の上位、下位のアドレスレジスタ、22はエリヤセンサ2cのセル(受光部)にチャージされた容量の充放電時間を制御するレジスタである。

【0035】23は外部装置とのデータの入出力を行うデータバスポート又はシリアルポートを示す。23に接続した2dは図1(b)に示した入出力ポートのハードウェア、端子部材である。24はキャッシュメモリ、及びRAMを示す。2bより入力した指紋パターンは21、22のレジスタの作用によって、瞬時に読み取って24のキャッシュメモリに一時貯える。

【0036】24はキャッシュメモリとRAMより構成したメモリ領域である。25はROM、フラッシュメ

モリより成るメモリ領域で電源がダウンしても中にある情報、データは消えない。しかし先にも説明したようにカードの使用期限に達したら25のデータ、情報は自動的に破壊する。従って25のROM領域もEEROMであれば電気信号によって消去できる。フラッシュメモリも同様である。

【0037】26はタイマー、カウンターで複数チャネルより構成している。エリヤセンサ2bより入力した指紋パターンを24のRAM上に貯えてある。所定時間経過のカウントを26のカウンターで行う。所定時間経過後、例えば5分とか10分間の経過後カウンターは消却信号をCPU100により出力する。

【0038】さらに26のタイマー、カウンターはカードの使用期限のカウントを行う。所定期間、例えば3年とか5年とか経過後同様に24、25のメモリ上のデータ、情報を消去するとCPU100自体も最終的に全ての機能を破壊する。カードの寿命をカード自身の機能によって全うする機構を備えている。

【0039】27はA/D変換器で、2bからの指紋パターンをデジタル情報に変換して24のキャッシュメモリに直ちに貯えられる。そして、25のROM上に登録してある本人認証パターンと照合する。本人認証指紋パターンはシステムによってはカード内のメモリにおかず決済の時に公衆回線を介してカード会社、銀行のデータベースからポート23を介して入力する。データベースより入力した本人認証パターンと使用時に入力した指紋パターンの照合をCPU100によって行う。

【0040】あるいはカードの構成をより単純化するために、カード上に、今入力した指紋パターンを外部装置とのインターフェース23を介して、データベースに送って、カード会社、銀行等のデータベースセンターでこれらの処理を行っても良い。登録してある指紋パターンとカード上から入力した指紋パターンが不一致の場合、複数回のくり返し入力を決済端末機より音声、表示によって使用者に指示する。

【0041】複数回行っても不一致の場合は、カードを没収したりカード内の機能によって、又はデータベースセンターより信号を発生してカード上のCPUをはじめ全ての機能を破壊して再度の使用を不可能にする。

【0042】28はD/A変換器で、カード内で演算した結果をアナログ出力したり、電子財布図4、41に示すようなケースに電子マネーカードを入れると残高、及び個人情報が表示される。このようなデジタル情報を数字又は文字で表示するためにアナログに変換する。

【0043】29は乗算器で、指紋パターンの入力データと本人認証の照合をすばやく行うための演算を行う。

当然100のCPUの指示によって処理実行を行う。100はCPUで8ビット又は16ビット程度のCMOS低消費電力型のものを使用する。101はシステムバスでワンチップCPU図1(b)の2cにおいて同一

ウエハー上に実装している。

【0044】図3は本カードを使用する環境のシステム構成を示す。公衆網31を介してカード決済センター32、銀行、デパート、スーパーマーケットなど大型店舗を示す35、小形店舗、街角にある端末機37、38はスマートオフィス、ホームオフィス等を示す。39はごく一般の家庭を示す。ここでは電話器FAX付の決済端末機110を特徴とする。

【0045】カード決済センター32は銀行等の金融機関、クレジットカード会社に設置してある。33は各種データ、情報の処理を行うサーバ、34はパスワード、指紋パターン等個人情報の格納を行うデータベースを示す。113は公衆回線112と接続分配するルータ、111はLANを示す。

【0046】35の銀行、大型店舗、大オフィス等においては公衆回線112を介して高速LAN111をはじめぐらせて、お客様の対応に答える。高速LANは少なくとも100Mbps以上のスピードをもっている。

36はATM(自動金銭処理機)又はカードリーダ等の決済端末機を示す。

【0047】37は比較的小型店舗、街角におかれたカードリーダ(決済端末機)を示す。この場合は公衆回線112より直接接続している。38はスマートオフィス、ホームオフィスを示す。サーバ33、決済端末機36より構成する。一般家庭及ホームオフィスにおいてもサーバ、パソコン33を複数台使用する場合も多くなってきた。ルータ113を介して、LAN111で家庭内の各部屋を結んで使用する場合もある。ルータ111は近年、家庭用のものも出回っている。

【0048】39は一般家庭、普通の家庭を示す。電話器110と決済端末機36が1体となった安価な構造のカードリーダを備えた。この装置があれば1台で電話、FAX機能と決済機の機能が使用出来て一挙両得となる。家庭からのホームショッピング、銀行決済等が可能となって、わざわざ銀行、郵便局に出かけなくとも用は足りる。高齢化社会に必携となるツールになるに違いない。

【0049】公衆網31は通常の電話網PSTNの他に21世紀初めに実用化するGII(Global Information Infrastructure)を基幹とする、ATM網、B-ISDNが主流となって高速化が実現する。

【0050】図4は電子財布と言うべきカードのケースを示す。41はカードを収納ケースで42は液晶等で構成した表示部を示す。43はスイッチで、ONすると42にカードの個人情報、銀行カード、電子マネーであれば残高が表示される。

【0051】カード内の情報、残高を表示させる場合、スイッチ43のONだけでなくカード1上に指紋捺印して、カード内に登録した指紋パターンに一致しない場合

は表示しない。電子財布41にカードと同様に図示しない指紋捺印部を設けて、カード上に登録してある指紋パターンと照合して、一致したときのみ、個人情報、残高等を表示して安全性を確保しても良い。カードと同様に電子財布41を落として他人に拾われても悪用される心配はない。

【0052】電子財布41の図示しない指紋捺印部の指紋パターンは、所定の時間経過と共に、又は所定時間個人情報を表示したらカードと同様に自動消去する。

10 これら機能及び電源はカード内の処理機能によって行われる。41には図示しないカードとの接触端子があってこれよりカードから電源と情報を入力する。41はワイヤレスのポケットに入る程度の大きさで良い。

【0053】電子財布41は、近年普及の著しい図示しないPDA(携帯情報端末器)と1体となった構造にしても良い。PDAのPIM(個人情報)と共にさらに使い勝手は向上する。

【0054】  
【第2の実施形態】図5は第2の実施形態によるカードの構成を示す図である。ここではカードの構成51は、現在流通しているクレジットカードと遜色がない。

カード51上に指紋捺印部52があるだけで、暗証番号の記憶部は従来のカードと同一である。

【0055】指紋捺印部52は図1(b)の2aと同様に指紋のパターンが乗り易い部材で構成している。図1(a)の2の指紋捺印部は背面に1体に構成したエリアセンサー図1(b)の2bによって読み取るために透明でなければならないが、52は必ずしも透明である必要はない。指紋パターンが乗り易い部材であれば良い。

【0056】当然、読み取り装置は図1の構造とは全く異なる。図6は読み取り装置(カード決済端末機)を示した図である。61は読み取り装置の全体図を示す。62はカード51上の指紋捺印部52を照射する光源。ここではLED(発光ダイオード)を使用した例を示した。指紋パターンを高率良く反射又は、透過する波長を発光する光源が最適である。

【0057】光源はLED、半導体レーザ、キセノンランプ、蛍光灯、EL等、効率良く指紋パターンを反射又は透過する波長を発生する安価で、小型のものを備えれば良い。

【0058】63はラインセンサで、CMOS、CCD(Charge Coupled Device)を使用する。カード51は指紋読み取り、カード清浄部66の中を移動するのでここではエリアセンサでなく安価なラインセンサで構成しても良い。

【0059】従来のクレジットカードと同様にカード51上にある暗証番号を66を移動中に読み取る機能を備えている。暗証番号は決済装置のキーボード、タッチキー上から使用者が入力するのも従来通りである。暗証番号の読み取り部は図示しないヘッド、又はカード5

1に埋込まれたC P Uより同様に図示していない6 6にある電気的な接触部から読み取る。

【0060】6 4, 6 5は清浄部である。カード5 1上の指紋捺印部5 2の清浄を行う。6 4は清浄ローラで6 5は清浄液を補給する容器を示す。6 4のローラは柔らかいゴム等で構成して読み取った後の指紋捺印部5 2を清浄して指紋パターンの消去を行う。

【0061】読み取った指紋パターンは本人認証の登録指紋パターンは5 1のカード上には記録されてなく、図3に示してある3 2のデータベース3 4に登録してある。使用方法は図3のシステム構成と同様である。

【0062】ただ図1、1のカードと異なり捺印した指紋を所定時間経過後に消去する機能はない。決済時に消去する安価で容易なカード構成であるのが特徴である。

【0063】又6 2、6 3による指紋パターン読み取り部は透過型でも良い。この場合5 2の捺印部は透明な部材を用いる。

【0064】以上述べた様に21世紀の電子マネー時代に備え、他人の無断使用、盗用、悪用を防ぐのと、職場、店舗、街角で、それに家庭からでも決済可能なカードを提供する事によって利便性の向上を目的としたものである。

#### 【0065】

【発明の効果】以上説明したように、本発明によれば以上のような効果を奏する。

【0066】カード上に捺印した指紋パターンと登録してある本人確認用指紋パターンを照合して、かつ從来からある暗証番号と併用することによって、本人認証の精度と安全性を向上させる事。

【0067】カード上に捺印した指紋パターンは所定時間経過後、又は決済時に自動消去して悪用を防ぐ事。

【0068】本人認証の安全性と精度を向上してあるから、家庭においても電話器と併用して電子決済が可能である。

#### 【0069】

##### 【図面の簡単な説明】

【図1】本実施形態による電子カードの全体を示す図である。

【図2】本実施形態における電子カードのシステム構成を示す図である。

【図3】本実施形態における使用環境を示すシステム構成図である。

【図4】本実施形態による電子財布の全体を示す図である。

##### 【図5】第2の実施形態によるカードの全体を示す図である。

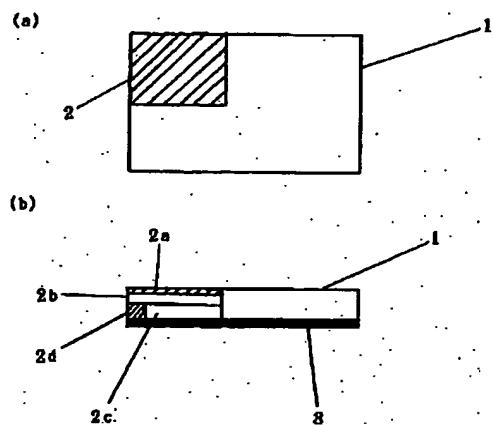
ある。

【図6】第2の実施形態によるカード読み取り装置を示す図である。

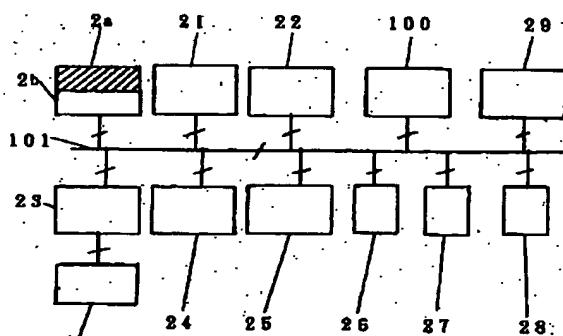
##### 【符号の説明】

1	電子カード
2	指紋読み取り部
2a	指紋捺印部
2b	半導体エリヤセンサー
2c	制御用L S I
10	2d 外部装置インターフェース部
	3 フィルム電池
	21, 22 レジスター
	23 データバス／シリアルポート
	24 キャッシュメモリ／RAM
	25 フラッシュメモリ／ROM
	26 タイマー／カウンター
	27 A／D変換器
	28 D／A変換器
	29 乗算器
20	31 公衆網
	32 カード決済センター
	33 サーバ
	34 データベース
	35 銀行、スーパー・マーケット、大オフィス
	36 ATM／決済端末機
	37 店舗、街角ターミナル
	38 スモールオフィス、ホームオフィス
	39 家庭
30	41 電子財布
	42 表示部
	43 スイッチ
	51 第2の実施形態によるカード
	52 第2の実施形態による指紋捺印部
	61 カード読み取り装置
	62 発光ダイオード
	63 CCDラインセンサー
	64 清掃ローラ
	65 清掃液容器
	66 カード移動部
40	100 C P U
	101 アドレス、データバス
	110 カード決済機付電話器
	111 LAN
	112 公衆回線
	113 ルータ

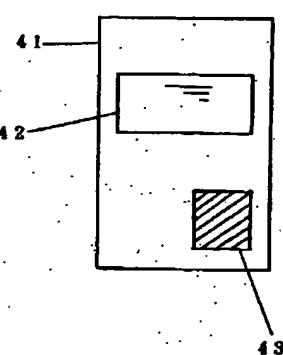
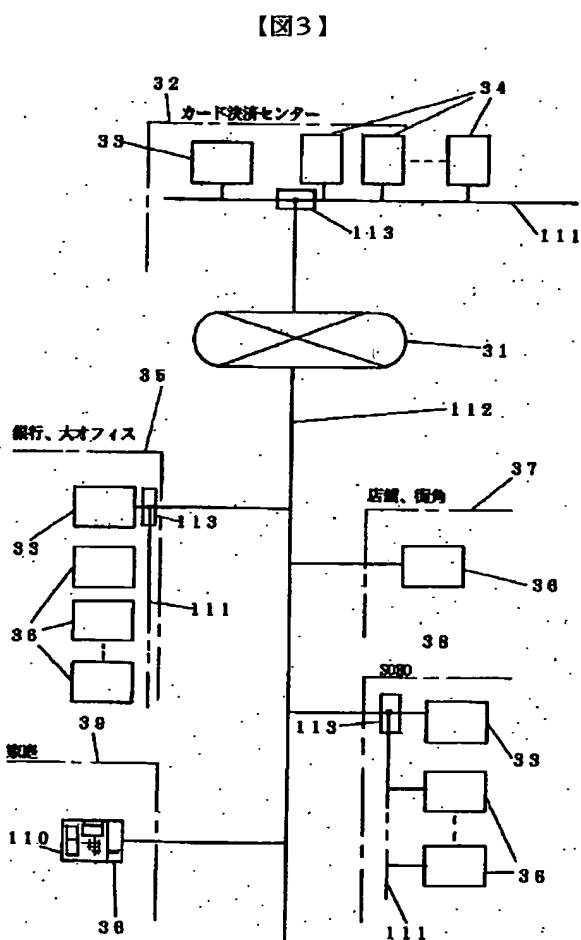
【図1】



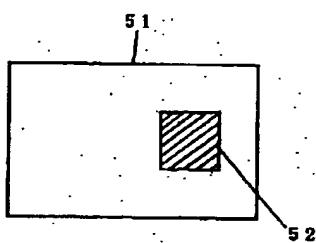
【図2】



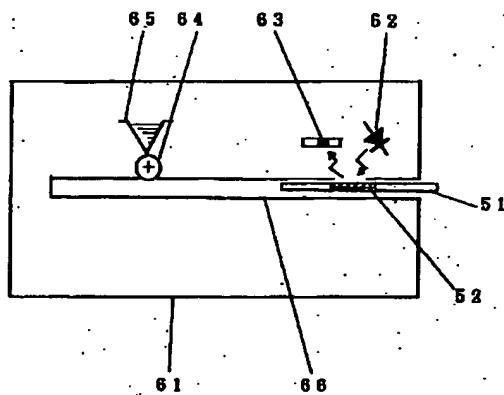
【図4】



【図5】



【図6】



---

フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テマコード(参考)

)

G 06 K 19/077

G 06 F 15/64

G

G 06 K 19/00

K

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**